## WHAT IS CLAIMED IS:

- 1. Automatic test equipment for testing non-deterministic packet data from a device-under-test, the automatic test equipment including:
  - a memory for storing expected packet data;
  - a receiver for receiving the packet data from the device-under-test; and
- a data validation circuit coupled to the receiver for validating the nondeterministic packet data based on the expected packet data from the memory.
- 2. Automatic test equipment according to claim 1 wherein the non-deterministic packet data validation circuit includes:
- a first-in-first-out circuit having an input coupled to the receiver and an output; and
- a comparator having a first input coupled to the first-in-first-out circuit and a second input coupled to the memory, the comparator operative to compare the first-in-first-out output to the expected packet data from the memory.
- 3. Automatic test equipment according to claim 2 and further including: a filter having an input coupled to the memory and an output coupled to the comparator second input, the filter configured to mask idle packet data.
- 4. Automatic test equipment according to claim 1 wherein the memory expected packet data includes predetermined signatures representing valid packet data combinations from the device-under-test, the non-deterministic packet data validation circuit including:
- a signature generator for creating actual signatures based upon actual data combinations received from the receiver; and
- a comparator for comparing the actual signatures to the predetermined signatures to identify valid packet data.
- 5. Automatic test equipment according to claim 4 and further including: a capture memory coupled to the receiver for storing the packet data received by the receiver.

- 6. Automatic test equipment according to claim 4 wherein the signature generator comprises a CRC arithmetic register.
- 7. Automatic test equipment according to claim 6 wherein the CRC arithmetic register comprises a linear feedback shift register.
- 8. Automatic test equipment for testing non-deterministic packet data from a device-under-test, the automatic test equipment including:

means for storing expected packet data;

means for receiving non-deterministic packet data from the deviceunder-test; and

means for validating non-deterministic packet data based on the expected packet data from the vector memory.

- 9. Automatic test equipment according to claim 8 wherein the means for validating includes:
- a first-in-first-out circuit having an input coupled to the receiver and an output; and
- a comparator having a first input coupled to the first-in-first-out circuit and a second input coupled to the means for storing expected packet data, the comparator operative to compare the first-in-first-out output to the expected packet data from the means for storing expected packet data.
- 10. Automatic test equipment according to claim 8 wherein the means for storing expected packet data includes means for storing predetermined signatures representing valid packet data combinations from the device-under-test, the means for validating including:

means for generating a signature based upon actual data combinations received from the receiver; and

means for comparing the actual signatures to the predetermined signatures to identify valid packet data.

11. Automatic test equipment according to claim 8 and further including: means for capturing the actual data from the receiver.

10

5

12. Automatic test equipment according to claim 10 wherein the means for generating a signature includes:

a CRC arithmetic register.

13. Automatic test equipment according to claim 12 wherein the CRC arithmetic register comprises:

a linear feedback shift register.

test; and

5

14. A method for testing non-deterministic packet data using automatic test equipment having a memory for storing expected packet data, the method including the steps:

receiving actual non-deterministic packet data from a device-under-

validating the non-deterministic packet data based on the expected packet data from the memory.

15. A method according to claim 14 wherein the validating step includes: pipelining the received data such that the first packet received is the first packet validated;

comparing, in the order received, each actual packet to the stored expected paket data in the memory; and

validating the non-deterministic packet data based on the comparing step.

16. A method according to claim 15 wherein the expected data includes idle data, the method further includes the step:

filtering the idle data to generate filtered expected data, and wherein the comparing step includes comparing, in the order received, each actual packet to the filtered expected data. 17. A method according to claim 11 wherein the memory stores predetermined valid signatures representing valid packet data combinations from the device-under-test, and wherein the validating step includes:

generating an actual signature for each received data packet;
comparing the generated actual signature to the predetermined valid
signatures; and

determining whether the received data packet passed or failed based on the comparison of the signatures.

18. A method according to claim 17 wherein the step of generating an actual signature includes:

calculating a checksum from the received packet data.

19. A method for validating non-deterministic packet data from a deviceunder-test using automatic test equipment, the automatic test equipment having a memory, the method including the steps:

establishing a library of known passing/failing signatures in the

5 memory;

15

testing the device-under-test;

generating a signature of actual data captured during the testing step; comparing the generated signature from the captured data to the library of known passing/failing signatures;

determining a pass/fail result for the device test if the compared signature matches a signature in the library;

evaluating the captured data to determine whether the device passed/failed if the compared signature does not match the library;

generating a new signature for the evaluated captured data; and adding the new signature to the library of known passing/failing signatures.